ICCWS 2023

18th International Conference on Cyber Warfare and Security

9 -10 March 2023, Towson, Maryland, USA

Mini Track on Legal and Security Challenges of Drone's Application in Military and Civilian Domains

Mini Track Chair: Dr. Pardis Moslemzadeh Tehrani, Faculty of Law, University of Malaya, Malaysia

The usage of drones/Unmanned Aerial Vehicles (UASs) has increased exponentially with the continuous rise of multi-purpose applications in military and civilian domains by amateurs, journalists, businesses, and governmental actors. Such activities led to the production of a large amount of private or sensitive imagery and an uncountable accumulation of data. UASs enable authorities to gather associated data along with imagery such as GPS coordinates of imagery or network traffic. It is necessary for states to develop a regulatory structure for the usage of UASs as by 2025 the jobs created from the data gathered by UAS operations which have an economic impact of $82 billion. The emerging threats of using drones along with counter-measures strategy needs to be investigated. The risk of hacking and hijacking drones could cause data breaches while posing a major risk to public safety. Malicious actors can hack drones and perform nefarious actions. Therefore, the need for detective, protective and preventive counter-measures is highly required.

Cyber-security risks may arise when using radiofrequency spectra to communicate between the drone's ground control and the drone platform, and between instruments on the drone such as cameras and data receivers. Drones are therefore vulnerable to hacking, interceptions and signal manipulation during flight. It also may infringe the right to privacy and private life if the drone is flown intrusively.

Various warning issued by states indicates that entities around the globe are taking to address the dangers posed by to airspace safety. Many countries including the USA developed national airspace drone traffic to manage the drone's flight. The government working hard to ensure providing better protection for people against emerging drone threats. Drones produce challenges for law enforcement as they can identify and interdict illicit activity. Giving the rapid technology advancement and proliferation, the government must address the fact that drones can be used maliciously to damage infrastructure, disrupt activities and hurt people.Topics of interest include, but are not limited to:

- Offensive and defensive usage of Drone/ UASs
- Legal and technical challenges of using Drone/ UASs
- Data breach of Drone/ UAS
- Cyber security in Drone/ UAS
- Collection, use, retention, and dissemination of data in Drone/ UAS
- Liability for cybersecurity negligence or data breaches in Drone/ UAS operations
- Cyber-attack directed at use of Drone/ UASs
- Regulatory aspects of Drone/ UAS

Dr. Pardis Moslemzadeh Tehrani, is a Visiting Associate Professor at the Faculty of Law, the University of Malaya. She was a Senior Lecturer at the same university from 2015 to 2022. Her research interests span the area of Information Technology Law, International Humanitarian Law and legal research methodology. Pardis has made scholarly contributions in peer-reviewed journals and presented papers in several national and international conferences and served on many conferences and workshop program committees.

Submission Details

In the first instance a 300-350 word abstract is required, to be received by the **31st August 2022**.

Submissions must be made using the online submission form at http://www.academic-conferences.org/conferences/iccws/iccws-abstract-submission/

If you have any questions about this track please email: pardismoslemzadeh@um.edu.my

See more about ICCWS 2023 at http://www.academic-conferences.org/conferences/iccws